SEMINAR WORKSHOP FORUM
15 October 1984
"Revisions to BISM - Effects on Personnel Security"

BLUE TEAM

STAT

Main concern was the BYA versus the proximity. Did not
have a thorough understanding of proximity as opposed to
BYA. Need more definition. Is BYA appropriate for
[   ] Would think not, at least not without
further processing.

GOLD TEAM

Also concerned about BYA and proximity accesses. Were
concerned about people moving around through an
organization with a proximity access, and you would not
know what access they had until they told you. How would
you handle that problem?

Who would decide what person got which briefing? Would we
coordinate with COTR to determine the degree of how much
that person is told?

What do you tell a person when they are debriefed?

GREEN TEAM

Were concerned about [   ] applicability
to BYA and Proximity accesses.

STAT

Regarding travel to denied areas--believe that the spouse
plays an important part. (Reporting of individual
travelling as well as spouse of accessed individual)

RED TEAM

Regarding pre-employment and post-employment screening--who
do you submit? What about your screening process? What
criteria do you follow? What length of time should be
involved?

Regarding foreign travel: All employees having accesses
are responsible for watching each other. They should be
sure all travel to denied areas is reported.

SEMINAR WORKSHOP FORUM
16 October 1984
"Industrial Security Audit Process"

GOLD TEAM

Discussed time it took to get our recommendations back to the contractor; what takes place in an audit.

BLUE TEAM

Conclusions:

Healthier relationship between contractor and auditor.

Enjoying increased support for security concerns as a result of the audit.

Auditors can emphasize to management those security concerns the CSO has traditionally had difficulties getting support on, thereby strengthening the CSO's position.

Audit helps clear out the "packrats" (at least temporarily).

Auditors provide a "fresh look".

Learn to be a partner with your COSR.

Security education is a big concern at contractor facilities: suggest getting help from program managers.

GREEN TEAM

Conclusions:

Recommendations come in two forms: Requirements and enhancements.

Observed that many companies present had never been audited. Suggested initial audits for these companies as a way of letting them know how they are doing and let them see their COSRs more.

Would like to see parallelism between the program office and the security office.

90 percent of problems were in the document control area.

RED TEAM

Red team composed mainly of persons new to audit experience. Were briefed on the procedures.

SEMINAR WORKSHOP FORUM
15 October 1984
"Revisions to BISM - Effects on Personnel Security"

BLUE TEAM

STAT

Main concern was the BYA versus the proximity. Did not
have a thorough understanding of proximity as opposed to
BYA. Need more definition. Is BYA appropriate for
[   ] Would think not, at least not without
further processing.

GOLD TEAM

Also concerned about BYA and proximity accesses. Were
concerned about people moving around through an
organization with a proximity access, and you would not
know what access they had until they told you. How would
you handle that problem?

Who would decide what person got which briefing? Would we
coordinate with COTR to determine the degree of how much
that person is told?

What do you tell a person when they are debriefed?

GREEN TEAM

Were concerned about [   ] applicability   STAT
to BYA and Proximity accesses.

Regarding travel to denied areas--believe that the spouse
plays an important part. (Reporting of individual
travelling as well as spouse of accessed individual)

RED TEAM

Regarding pre-employment and post-employment screening--who
do you submit? What about your screening process? What
criteria do you follow? What length of time should be
involved?

Regarding foreign travel: All employees having accesses
are responsible for watching each other. They should be
sure all travel to denied areas is reported.

SEMINAR WORKSHOP FORUM
16 October 1984
"Industrial Security Audit Process"

GOLD TEAM

Discussed time it took to get our recommendations back to the contractor; what takes place in an audit.

BLUE TEAM

Conclusions:

Healthier relationship between contractor and auditor.

Enjoying increased support for security concerns as a result of the audit.

Auditors can emphasize to management those security concerns the CSO has traditionally had difficulties getting support on, thereby strengthening the CSO's position.

Audit helps clear out the "packrats" (at least temporarily).

Auditors provide a "fresh look".

Learn to be a partner with your COSR.

Security education is a big concern at contractor facilities: suggest getting help from program managers.

GREEN TEAM

Conclusions:

Recommendations come in two forms: Requirements and enhancements.

Observed that many companies present had never been audited. Suggested initial audits for these companies as a way of letting them know how they are doing and let them see their COSRs more.

Would like to see parallelism between the program office and the security office.

90 percent of problems were in the document control area.

RED TEAM

Red team composed mainly of persons new to audit experience. Were briefed on the procedures.

Next 1 Page(s) In Document Exempt

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Seminar Workshop Discussions

STAT FROM:

C/Industrial Security Branch/OS

STAT

EXTENSION	NO.
	DATE 7 November 1984

TO: (Officer designation, room number, and building)	DATE		OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
	RECEIVED	FORWARDED		
1. C/SS/OD&E				0-1: Attached notes reflect issues and questions raised by the four contractor teams during the workshop wrap up presentations at the Industrial Security Seminar Workshops held on 15 and 16 October 1984. Items on page one indicate fuzzy areas regarding the recent revisions to the BISM. These concerns are being forwarded to you for your information and any action you deem appropriate. Items on page two relate to the Industrial Security Audit Process which ISB will address, as appropriate, in the scheduling and actual conduct of the Industrial Security Audits.
2.				
3.				
4.				
5.				
6.				Representatives of the four contractor teams are identified on paper attached to page one.
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

STAT

FORM 610 USE PREVIOUS EDITIONS
1-79